Translating $I\Delta_0$+exp proofs into weaker systems

Chris Pollett

Department of Mathematics,
University of California, Los Angeles, 90095-1555 CA
cpollett@willow.math.ucla.edu

The purpose of this paper is to explore the relationship between $I\Delta_0$+exp and its weaker subtheories. We give a method of translating certain classes of $I\Delta_0$+exp proofs into weaker systems of arithmetic such as Buss' systems S_2. We show if $IE_i(exp) \vdash A$ with a proof P of $expind\text{-}rank(P) \leq n+1$ where all ($\forall \leq$: right) or ($\exists \leq$: left) have bounding terms not containing function symbols then $S_2^i \supseteq IE_{i,2} \vdash A^n$. Here A is not necessarily a bounded formula. For $IOpen(exp)$ we prove a similar result. Using our translations we show $IOpen(exp) \subsetneq I\Delta_0(exp)$. Here $I\Delta_0(exp)$ is a conservative extension of $I\Delta_0$+exp obtained by adding to $I\Delta_0$ a symbol for 2^x to the language as well as defining axioms for it.

Key words: bounded arithmetic, complexity theory, interpretation, separations
1991 MSC: 03F30, 68Q15

1 Introduction

Of the commonly studied bounded arithmetic theories $I\Delta_0$+exp, the theory with induction for bounded formulas in the language of 0, S,+,$\cdot$ together with the axiom saying the exponential function is total, is one of the more interesting. It is one of the weakest fragments of arithmetic known to prove the Matiyasevic Robinson Davis Putnam Theorem (MRDP) Theorem that every Σ_1-formula is equivalent to an $\exists_1$-formula [6]. It is also known to be both finitely axiomatized [15] and equivalent to its IE_1+exp fragment [8]. In contrast the bounded arithmetic theories $I\Delta_0$ and $I\Delta_0$+Ω_1 (equivalent to Buss' S_2), which have induction on formulas involving only sub-exponential growth rate functions are not known to prove the MRDP or known to be finitely axiomatized. In fact, if either of these is provable in $I\Delta_0$+Ω_1 then it would imply collapse of the polynomial hierarchy. Thus, it is important to study $I\Delta_0$+exp to see how well proof techniques for this theory can be transferred to weaker theories.

Wilkie-Paris [15] have shown several interesting connections between $I\Delta_0{+}exp$ and weaker theories. They have shown $I\Delta_0{+}exp$ cannot prove $Con(Q)$ and $I\Delta_0{+}exp$ proves $(\forall x)A$ where A is bounded iff $Q{+}(\forall x)A$ is interpretable in Q. These results would seem to indicate that $I\Delta_0{+}exp$ is not too far in strength from $I\Delta_0$. On the other hand, they show $I\Delta_0{+}exp$ is not interpretable in Q; whereas, $I\Delta_0$ and S_2 are known to be. Further $I\Delta_0{+}exp$ can give a truth definition for bounded formulas in the language L_2 as well as prove a partial cut-elimination result. It is, thus, able to prove the bounded consistency, and hence also free-cut-free consistency, of S_2 and so is in some sense quite a bit stronger than S_2.

Despite the fact that $I\Delta_0{+}exp$ is not interpretable in $I\Delta_0$, it is known if $I\Delta_0{+}exp$ proves $(\forall x)A(x)$ where A is a bounded formula then $I\Delta_0$ proves $(\forall x)((\exists y)(y = 2^x_k) \supset A(x))$. Here 2^x_k is a stack of 2's k high with an x at the top. This result has both a simple compactness argument proof [7] as well as a proof using Herbrand's theorem [4] which could in principle be used to give a bound on k in terms of the maximum nesting depths of exp in the $I\Delta_0{+}exp$ proof. Intuitively, this result says: given x, if $I\Delta_0$ knows a big enough y exists then it can show $A(x)$ holds. Or said another way, if x is very small then $I\Delta_0$ should be able to prove $A(x)$. This result is interesting in that it gives us some information about how results in $I\Delta_0{+}exp$ translate into weaker theories.

Motivated by this result, in this paper we reformulate the theory $I\Delta_0{+}exp$ by expanding the base language of $I\Delta_0$ with a new symbol 2^x and adding to $I\Delta_0$ two open axioms for 2^x. This conservative extension of $I\Delta_0{+}exp$ is called $I\Delta_0(exp)$. We consider translations of formulas in this language into formulas in weaker theories based on the map $x \rightarrow |x|_n$ where $|x|_n$ is the length function ($\lceil \log_2(x+1) \rceil$) applied n times to x. The precise definition of our translations is closely related to the RSUV-translation of second-order bounded arithmetic theories [14]. We show that if $IE_i(exp)$ proves A with a proof P in which no function symbols appear in bounding terms of ($\forall \leq$: right) or ($\exists \leq$: left) inferences then there is an $n \leq exp\text{-}rank(P) + 1$ such that IE_i^m proves the translation A^{n+m}. Here IE_i^m is the theory with E_i-induction up to terms of the form $|s|_m$ in the language L_2. When $m = 0$ we get the theory with usual E_i-induction in L_2. We are saying $IE_i(exp)$ proof rather than $I\Delta_0(exp)$ proof since it is unclear if $IE_i(exp)$ can prove the MRDP theorem without using ($\forall \leq$: right) or ($\exists \leq$: left) inferences with bounding terms containing function symbols. The reason why we are interested in such weak theories is that recently it has been shown that when $m - i \geq 4$ these theories cannot prove the collapse of the polynomial hierarchy [10].

We hope our translations might be useful for separation results. To see that this may be possible, in this paper we show $IOpen(exp) \subsetneq I\Delta_0(exp)$. This is done by showing if $IOpen(exp)$ proves an open formula A with free-cut free proof P, then there is an $n \leq exp\text{-}rank(P){+}1$ such that $IOpen$ proves A^n. We

use this to show $I\Delta_0(exp) \vdash FCFCon(IOpen(exp))$. Since $I\Delta_0(exp)$ does not prove its own free-cut-free consistency this gives the result. Shepherdson [13] has noted that $IOpen(exp)$ can prove the irrationality of $\sqrt{2}$, which is not provable in $IOpen$. This indicates $IOpen(exp)$ may be substantially stronger than $IOpen$ which has recursive models. As far as the author knows it is still open if $IOpen(exp)$ has recursive models. It is known by Wilmers [16] that IE_1 does not. We show $IOpen(exp)$ is not equal to $I\Delta_0{+}exp$ also holds if one adds new function symbols and axioms that respect our translation and if the theory that is translated to is in interpretable in Q.

We now discuss the organization of this paper. In the next section we give the background needed to understand the rest of the paper. In the third section, we give our translation.

2 Preliminaries

We will work in the language L_2 which contains the non-logical symbols: 0, S, $+$, $\cdot$, $\leq$, $\dot{-}$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $MSP(x,i)$ and $\#$. The symbols 0, $S(x) = x+1$, $+$, $\cdot$, and $\leq$ have the usual meaning. The intended meaning of $x \dot{-} y$ is x minus y if this is greater than zero and zero otherwise, $\lfloor \frac{1}{2}x \rfloor$ is x divided by 2 rounded down, and $|x|$ is $\lceil \log_2(x+1) \rceil$, that is, the length of x in binary notation. $MSP(x,i)$ stands for 'most significant part' and is intended to mean $\lfloor x/2^i \rfloor$. Finally, $x\#y$ reads 'x smash y' and is intended to mean $2^{|x||y|}$. The language L_1 is the language $L_2 \backslash \{\#\}$. We call a quantifier of the form $(\forall x \leq t)$ or $(\exists x \leq t)$ where t is an term in the language not containing x a *bounded quantifier*. A formula is *bounded* or Δ_0 if all its quantifiers are. A quantifier of the form $(\forall x \leq |t|)$ or of the form $(\exists x \leq |t|)$ is called *sharply bounded* and similarly a formula is *sharply bounded* if all its quantifiers are.

Given a language L, we define a hierarchy of formulas $E_{i,L}$ and $U_{i,L}$ as follows: $E_{1,L}$ are those formulas of the form $(\exists x \leq t)\phi$ and $U_{1,L}$ are those formulas of the form $(\forall x \leq t)\phi$ where ϕ is an open formula. $E_{i,L}$ are those formulas of the form $(\exists x \leq t)\phi$ where $\phi \in U_{i-1,L}$-formula. $U_{i,L}$ are those formulas of the form $(\forall x \leq t)\phi$ where $\phi \in E_{i-1,L}$. We will write E_i and U_i when the language is understood. By a *bounded* or Δ_0-formula we mean an L-formula in which all the quantifiers are bounded. We write *open* for the class of quantifier-free formulas. For $i > 0$, we define a $\hat{\Sigma}^b_i$-formula (resp. $\hat{\Pi}^b_i$-formula) to be a E_{i+1}-formula (resp. U_{i+1}-formula) whose innermost quantifier is sharply bounded.

Next we define $BASIC$ to be axiomatized by all subtitution instances of a finite set of quantifier free axioms for the non-logical symbols of L_2. These axioms are listed in Buss [2] with the exception of the axioms for MSP and $\dot{-}$ which are listed in Takeuti [14]. We will take $BASIC_1$ to be the L_1-theory

axiomatized by $BASIC$ less the axioms not in L_1.

To present the rest of the theories we will be working with we first give some abbreviations of L_2-terms we will frequently use:

$$
\begin{aligned}
2^{|y|} = 2^{|y|^1} &:= 1\#y & \max(x,y) &:= cond(K_{\leq}(x,y), y, x)\\
2^{|y|^n} = 2^{1\cdot|y|^n} &:= 2^{|y|^{n-1}}\#y & \min(x,y) &:= cond(K_{\leq}(x,y), x, y)\\
2^{k\cdot|y|^n} &:= 2^{|y|^n}\cdot 2^{(k-1)\cdot|y|^n} & 2^{\min(|y|,x)} &:= MSP(2^{|y|}, |y| \dot{-} x)\\
K_{\neg}(x) &:= 1 \dot{-} x & LSP(x,i) &:= x \dot{-} MSP(x,i)\cdot 2^{\min(|x|,i)}\\
K_{\leq}(x,y) &:= K_{\neg}(y \dot{-} x) & cond(x,y,z) &:= K_{\neg}(x)\cdot y + K_{\neg}(K_{\neg}(x))\cdot z
\end{aligned}
$$

The k and n in $2^{k\cdot|y|^n}$ are fixed integers. Taking products of terms $2^{k\cdot|s|^n}$ we can construct terms representing $2^{p(|s|)}$ where p is any polynomial. For clarity, we write $2^{\ell(x)}$ for $2^{\min(|t(x)|,\ell(x))}$, if $\ell(x)$ is a term which is obviously less than $|t(x)|$ for some $t \in L_2$.

Definition 1 *$XBASIC$ is the theory obtained from $BASIC$ by adding the following axiom:*

$$a \leq |b| \wedge a \leq |c| \supset 2^{\min(|b|,a)} = 2^{\min(|c|,a)}.$$

The new axiom of $XBASIC$ will be useful for our translations of $I\Delta_0(exp)$ proofs. We will formalize $BASIC$ and $XBASIC$ proofs in the system LKB of Buss [2] where we have equality axioms and where we take the axioms of $BASIC$ ($XBASIC$) as initial sequents. The main point of LKB is it treats bounded quantifiers syntactically. We define stronger theories by adding various types of induction rules to $BASIC$ and $XBASIC$.

Definition 2 *A Ψ-L^mIND inference is an inference*

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(|t(x)|_m), \Delta}$$

where b is an eigenvariable and must not appear in the lower sequent, t is a term in the language, and $A \in \Psi$. Here $|a|_0 = a$ and $|a|_m = ||a|_{m-1}|$. We call $|t(x)|_m$ the principal term *of the induction inference.*

We often write IND, $LIND$ and $LLIND$ instead of L^0IND, L^1IND, and L^2IND.

Definition 3 *We define the theory $I\Delta_0$ to be $BASIC_1$+Δ_0-IND.*

We would like to point out that $I\Delta_0$ is usually defined in the language without $\dot{-}$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, and MSP; however, since these functions are all Δ_0-definable in the usual $I\Delta_0$ [3], our theory will be a conservative extension of that theory. The graph of $exp(x,y) := x^y$ is Δ_0-definable in $I\Delta_0$ [1,6]. Using this Δ_0-definition, we can define the define exp axiom $(\forall x)(\forall y)(\exists z)(z = exp(x,y))$. The theory $I\Delta_0$+exp is axiomatized by $I\Delta_0$ together with the exp axiom. The theory $I\Delta_0$+Ω_1 is axiomatized by $I\Delta_0$ together with the axiom $(\forall x)(\forall y)(\exists z)(z = exp(x, \log y))$.

Definition 4 $(i \geq 0)$ *The theory IOpen is the theory BASIC+open-IND. We define* IE_i^m *to be*

$$XBASIC{+}E_i\text{-}L^mIND$$

and we define S_2^i *to be* $BASIC{+}\hat{\Sigma}_i^b\text{-}LIND$ *and* T_2^i *to be* $BASIC_k{+}\hat{\Sigma}_i^b\text{-}IND$.

We write S_2 *for* $\cup_i S_2^i$.

We mention here that it is straightforward using *open-IND* to prove the new $XBASIC$ axiom, so $XBASIC \subseteq IOpen$. The theory S_2 is a conservative extension of the Wilkie Paris theory $I\Delta_0$+Ω_1 [15,9]. The sequent calculus system for the former theory is often more convenient than for the latter, although the latter theory does have the virtue of being defined over the same language as $I\Delta_0$+exp. The above axiomatization of S_2^i was given in Pollett [11] and shown to be equivalent to the original one given in Buss [2]. It is known from the latter reference that $S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$ and it follows from the above definitions that $S_2^{i-1} \subseteq IE_i^0 \subseteq T_2^i$. Thus, $S_2 = \cup_i IE_i^0$. We write IE_i^0 as IE_i.

Theorem 5 *If* $A(x)$ *is a* Ψ*-formula, and* $XBASIC \vdash t \leq |s|_m$ *for some term* s *then the inference*

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(t), \Delta}$$

is admissable in $XBASIC{+}\Psi\text{-}L^mIND$.

PROOF. Given that $XBASIC{+}\Psi\text{-}L^mIND$ proves $A(b), \Gamma \rightarrow A(Sb), \Delta$, it follows that it proves

$$A(\min(b, |s|_m)), \Gamma \rightarrow A(\min(Sb, |s|_m)), \Delta.$$

So by an L^mIND, $XBASIC{+}\Psi\text{-}L^mIND$ proves

$$A(\min(0, |s|_m)), \Gamma \rightarrow A(\min(t, |s|_m)), \Delta.$$

By induction on the complexity of A bit also proves $t \leq |s|_m, A(\min(t, |s|_m)) \rightarrow A(t)$ and $A(0) \rightarrow A(\min(0, |s|_m))$. Thus, performing the appropriate cuts the lower sequent can be derived. $\Box$

We conclude this section by defining a conservative extension of $I\Delta_0{+}exp$. Let L_{exp} be the language $L_1 \cup \{exp\}$. Define $BASIC(exp)$ to be $BASIC_1$ together with the two axioms: (1) $exp(0) = S0$ and (2) $exp(Sx) = exp(x)\cdot SS0$. We write $IOpen(exp)$, $IE_i(exp)$, and $I\Delta_0(exp)$ for $BASIC(exp){+}open\text{-}IND$, $BASIC(exp){+}E_i\text{-}IND$, and $BASIC(exp){+}\Delta_0\text{-}IND$ respectively. We state without proof the next theorem which is a result of Kaye [8].

Theorem 6 *$I\Delta_0(exp) = IE_1(exp)$ is a conservative extension of $I\Delta_0{+}exp$.*

We mention here that the relationship between $IOpen{+}exp$ and $IOpen(exp)$ is unclear. This is because the exp-axiom is not an *open*-formula so $IOpen{+}exp$ does not have induction for it. On the other hand, the $exp(x, y, z)$ holds iff there is a sequence w of length y such that the first item of w is x and $i + 1$st item of w is x time the ith item of w and the last item is z. This is an E_2-formula and it does not seem easy to prove such a sequence exists in $IOpen(exp)$. Since $IOpen(exp)$ allows induction on formulas with exp in it we feel it is the more natural theory and will use it for the remainder of this paper.

3 Main Results

Suppose a theory T in the language L_{exp} proves A with LKB-proof P. The $exp\text{-}rank(t)$ for $t \in L_{exp}$ is the maximum number of occurrences of exp in any branch of t viewed as a tree. The $exp\text{-}rank(P)$ is the maximum of the $exp\text{-}rank(t)$ for t appearing in P. The $expind\text{-}rank$ of P is the maximum $exp\text{-}rank(t)$ of t a principal term of an induction inference in P. We now define translations of L_{exp}-formulas into L_2-formulas for each integer n.

For $t \in L_{exp}$ we first define a term t^M. If t is 0 then t^M is 0, if t is a then t^M is a, if t is Sh or $exp(h)$ then t^M is $4\#h^M\#h^M$, if $t := h \circ s$ where $\circ$ is $+$ or $\cdot$ then t^M is $4h^M\#s^M$, and if $t := h \dot{-} s$ or $t := MSP(h, s)$, t^M is h^M. Now our translation t^n of t is constructed by replacing every variable a in t by $|a|_n$ and by replacing every occurrence of $exp(s)$ by $2^{\min(|s^M|, s^n)}$. Next $(s = t)^n$ is $s^n = t^n$ and $(s \leq t)^n$ is $s^n \leq t^n$. The translation commutes with the propositional connectives. For the quantifiers, we have two cases:

- If A is $(\forall x)B$ or $(\exists x)B$, then A^n is $(\forall x)B^n$ resp. $(\exists x)B^n$.
- If A is $(\forall x \leq t)B$ or $(\exists x \leq t)B$, and B^n is $\tilde{B}^n(|x|_n)$, then A^n is $(\forall x \leq t^n)\tilde{B}^n(x)$ resp. $(\exists x \leq t)\tilde{B}^n(x)$.

The following lemma can be proved by induction on the complexity of t:

Lemma 7 *Suppose $0 \leq m \leq n - exp\text{-}rank(t)$. Then $XBASIC$ proves $t^n \leq$*

$|t^M|_m$.

Theorem 8 *Suppose $IE_i(exp) \vdash A$ with an LKB-proof P. Further suppose all bounding terms t in ($\forall \leq$: right) or ($\exists \leq$: left) inferences in P do not involve function symbols. Let $n := \max(exp\text{-}rank(P), expind\text{-}rank(P) + m)$. Then $IE_i^m \vdash A^n$.*

PROOF. Let P^n denote the result of applying the translation $B \to B^n$ for every formula in P. We will convert P^n into a IE_i^m-proof. First, note substitution instances of axioms of Q or equality axioms in P will remain substitution instances axioms of Q or equality axioms in P^n. Next, consider the translation of an *exp*-axiom in P^n. *exp*-axiom (1) becomes $2^{\min(|0|,0)} = S0$ which is easy to prove in $XBASIC$. For *exp*-axiom (2), a translation would look like $2^{\min(|(St)^M|,St^n)} = 2^{\min(|t^M|,t^n)} \cdot SS0$. Since $exp\text{-}rank(t) < exp\text{-}rank(P) \leq n$, by Lemma 7, $XBASIC$ proves $t^n \leq |t^M|$. By the new axiom for $XBASIC$ we have

$$2^{\min(|t^M|,t^n)} = 2^{\min(|(St)^M|,t^n)}$$

since $XBASIC$ proves $t^n \leq |t^M| \leq |(St^M)|$. Now the axiom for MSP gives

$$MSP(2^{|(St)^M|}, (|(St)^M| \dot{-} t^n)) = \lfloor \frac{1}{2} MSP(2^{|(St)^M|}, |(St)^M| \dot{-} St^n) \rfloor.$$

i.e., $2^{\min(|(St)^M|,t^n)} = \lfloor \frac{1}{2} 2^{\min(|(St)^M|,St^n)} \rfloor$. So using the axioms for a half one can derive the translation of an *exp* axiom. We can thus add to P^n the appropriate $XBASIC$ proof to make a valid IE_i^m proof in this case.

One can verify that the only inferences in P^n that may not be valid IE_i^m inferences are translations of E_i-IND inferences, ($\forall \leq$: right) inferences, or ($\exists \leq$: left) inferences. Now consider the translation of a E_i-IND inference:

$$\frac{\tilde{B^n}(|b|_n), \Gamma^n \to \tilde{B^n}(S|b|_n), \Delta^n}{\tilde{B^n}(0), \Gamma^n \to \tilde{B^n}(t^n), \Delta^n}$$

B_n is an E_i-formula and so IE_i^m can prove $L^m IND$ for it. $XBASIC$ can prove $|Sb|_n = |b|_n \vee |Sb|_n = S|b|_n$. So from the upper sequent above IE_i^m can derive

$$\tilde{B^n}(|b|_n), \Gamma^n \to \tilde{B^n}(|Sb|_n), \Delta^n.$$

Since $exp\text{-}rank(t) + m \leq expind\text{-}rank(P) + m < n$, by Lemma 7, $XBASIC$ can prove $t^n \leq |t^M|_m$, so by Theorem 5 and since $|0|_n = 0$, $IE_{i,2}^m$ proves

$$\tilde{B^n}(0), \Gamma^n \to \tilde{B^n}(t^n), \Delta^n.$$

So to make P^n a valid proof in this case we incorporate the above sketched derivation. Now we must consider ($\forall \leq$: right) and ($\exists \leq$: left) inferences.

These are essentially treated in the same way so we only show the ($\exists \leq$: left) inference, a translation of which would look like:

$$\frac{|b|_n \leq \bar{t}^n, \tilde{B}^n(|b|_n), \bar{\Gamma}^n \rightarrow \bar{\Delta}^n}{\exists x \leq \bar{t}^n \tilde{B}^n(x), \bar{\Gamma}^n \rightarrow \bar{\Delta}^n}$$

We are assuming the bounding term t involved no function symbols. So t^n is really of the form 0 or $|c|_n$ for some variable n. We show the second case as the first one is relatively easy. Let d be a new variable not appearing in P^n. First, derive using equality axioms $d = |b|_n, \tilde{B}^n(d) \rightarrow \tilde{B}^n(|b|_n)$ and $d = |b|_n, d \leq t^n \rightarrow |b|_n \leq t^n$. Cutting these two sequents against the upper sequent, together with some structural rules, and an ($\exists$:left) inference gives $(\exists x)d = |x|_n, d \leq \bar{t}^n, \tilde{B}^n(d), \bar{\Gamma}^n \rightarrow \bar{\Delta}^n$. Now derive $d \leq |c|_n \rightarrow (\exists x)d = |x|_n$. We can prove this by making a L_2-term h such that $|h|_n = d$. h can be defined as a stack of $2^{\min}$'s n-high with $|d|_n$ at the top and where the second component in the *min* at the i level is $|c|_i$. Since $t^n = |c|_n$, using this sequent, a cut, and a contraction we get $d \leq t^n, \tilde{B}^n(d), \bar{\Gamma}^n \rightarrow \bar{\Delta}^n$ from which the lower sequent above follows by an ($\exists \leq$: left) inference. $\square$

We would like to specifically mention at this point what this result means for the well studied theories T_2^i and S_2^i of Buss [2].

Corollary 9 *Suppose $IE_i(exp) \vdash A$ with LKB-proof P. Further suppose all bounding terms t in ($\forall \leq$: right) or ($\exists \leq$: left) inferences in P do not involve function symbols. Let $n := \max(exp\text{-}rank(P), expind\text{-}rank(P))$. Then $T_2^i \vdash A^n$ and $S_2^i \vdash A^{n+1}$. Also, $T_2 = S_2 \vdash A^n$.*

PROOF. This follows from Theorem 8 since $IE_i \subseteq T_2^i$ and $IE_i^1 \subseteq S_2^i \subseteq S_2$. $\square$

For the next result we need a couple of definitions. A free cut is a cut on a formula B which is not directly descended from an axiom or a principal formula in an induction inference. A proof is *free-cut free* if it does not have a free-cut. It is a result of Buss [2] that since all of $IOpen(exp)$'s axioms are open and since the *open-IND* rule involves only open principal formulas, any $IOpen(exp)$ proof of an *open*-formula will contain only open formulas.

Theorem 10 *Suppose $IOpen(exp) \vdash A$ an open-formula with free-cut free proof P. Let $n := exp\text{-}rank(P)$. Then $IOpen \vdash A^n$.*

PROOF. The proof is essentially the same as Theorem 8. We do not have to worry about quantifier rules since a free-cut free proof of an *open*-formula in $IOpen(exp)$ will consist of only *open*-formulas. $\square$

4 Some separation results

In this section we will assume we have carried out a formalization of the syntax of bounded arithmetic proofs within $I\Delta_0{+}exp$. The reader is invited to consult Buss [2], Hajek and Pudlak [7], or Buss [3] for details on how this may be carried out. We write $ThmFCF_T(\ulcorner\phi\urcorner)$ for the formula which says "ϕ codes a formula which is a free-cut free theorem of theory T". We write $FCFCon(T)$ for the formula $\neg ThmFCF_T(\ulcorner 0 = 1\urcorner)$. It follows from Theorem 10 on page 144 of Buss [2] that $I\Delta_0{+}exp$ does not prove $FCFCon(I\Delta_0{+}exp)$. On the other hand, we will show below $I\Delta_0{+}exp$ does prove $FCFCon(IOpen(exp))$.

Lemma 11 *$I\Delta_0{+}exp$ proves $FCFCon(IOpen)$.*

PROOF. In view of Theorem 6 we can work in $I\Delta_0(exp)$. Theorem V.4.18 in Hajek and Pudlak [7] shows there is a Δ_0-formula $\mu_1(e, x, z)$ such that for every E_1-formula ϕ, $S^1_2 \vdash \phi \equiv \mu_1(\ulcorner\phi\urcorner, x, 2^{|x|^{\ulcorner\phi\urcorner}})$. Here $\ulcorner\phi\urcorner$ is an appropriate Gödel number for ϕ and we are assuming if ϕ is of arity greater than one we have done the appropriate pairing. Since $I\Delta_0(exp)$ can define $x\#y$ as $2^{|x||y|}$ this is provable in $I\Delta_0(exp)$. Also for y a variable, $I\Delta_0(exp)$ can define $2^{|x|^y}$. We define $VALID(e) := (\forall x)\mu_1(e, x, 2^{|x|^e})$. For any sequent of open formulas $A_1, \ldots A_n \to B_1 \ldots B_m$ we can view it as a single open formula $\wedge_i A_i \supset \vee_j B_j$. So we can define $\ulcorner A_1, \ldots A_n \to B_1 \ldots B_m\urcorner$ as $\ulcorner \wedge_i A_i \supset \vee_j B_j\urcorner$. Now for any $IOpen$ inference it is not hard to show if $I\Delta_0(exp)$ proves $VALID(\ulcorner\Gamma \to \Delta\urcorner)$ for each $\Gamma \to \Delta$ an upper sequent of open formulas in an $IOpen$-proof, then it can prove $VALID(\ulcorner\Lambda \to \Omega\urcorner)$ for the lower sequent. Using this $I\Delta_0(exp)$ can show for all e that $ThmFCF_{IOpen}(e) \supset VALID(e)$. In other words, $\neg VALID(e) \supset \neg ThmFCF_{IOpen}(e)$. Now $I\Delta_0(exp)$ proves $\neg(0 = 1)$, and hence, $\neg VALID(\ulcorner 0 = 1\urcorner)$ and $\neg ThmFCF_{IOpen}(\ulcorner 0 = 1\urcorner)$. This last is $FCFCon(IOpen)$. $\Box$

It seems harder to give a predicate of the form $VALID$ for $IOpen(exp)$ proofs in $I\Delta_0(exp)$, since the natural way to define the equivalent to μ_1 would involve stacks of 2's in the third component that grow with $\ulcorner\phi\urcorner$.

Theorem 12 *$I\Delta_0{+}exp$ proves $FCFCon(IOpen(exp))$. So $IOpen(exp) \subsetneq I\Delta_0(exp)$.*

PROOF. It is not hard to Δ_0-define a function which determines $n := \max(exp\text{-}rank(P), expind\text{-}rank(P) + 1)$ for an $IOpen(exp)$ proof P. Given this function $I\Delta_0{+}exp$ can define a function which translates an $IOpen(exp)$ proof P of A into an $IOpen$ proof of A^n for this n. To see this recall the folklore

result [5] that $I\Delta_0{+}exp$ can Δ_0-define any elementary function. In this case, the case the proof of Theorem 10 gives a translation which can be computed in polynomial time. Notice for any n our translation has $(0 = 1)^n := (0 = 1)$. The theorem then follows by Lemma 11 and Theorem 6. $\Box$

The above result relies on two things: (1) $I\Delta_0{+}exp$ can translate *open*-proofs in the theory with exp into *open*-proofs in the theory without exp and (2) $I\Delta_0{+}exp$ can prove the free-cut free consistency of the theory without exp. We cannot modify the above proof to show $I\Delta_0{+}exp$ proves $FCFCon(I\Delta_0(exp))$ since we have no means of translating a free-cut-free $I\Delta_0(exp)$ proof of $0 = 1$ where the bounding terms on ($\forall \leq$: right) or ($\exists \leq$: left) inferences may involve exp into an S_2 proof. Now suppose we introduce a new m-ary function symbol f to the language of L_{exp} and L_2 and define $IOpen(exp, f)$ and $IOpen(f)$ to be the theories obtained by allowing in the deductive system substitution instances of *open* defining axioms for f and allowing f to appear in *open*-$LIND$ inferences. Assume the *open*-defining axioms for f involve symbols other than exp and assume the resulting theory is consistent. We can extend our translations to f by defining

$$(f(t_1, \ldots, t_m))^n := f(t_1^n, \ldots t_m^n).$$

Lemma 13 *Suppose $IOpen(exp, f) \vdash A$ and open-formula with free-cut free proof P. Let $n := \max(exp\text{-}rank(P), expind\text{-}rank(P) + 1)$. Then $IOpen(f) \vdash A^n$.*

PROOF. Since any substitution instance of an *open*-axiom $A(a_1, \ldots, a_m)$ for f as an initial sequent in $IOpen$ proofs, $A(|b_1|_n, \ldots |b_m|_n)$ will be a valid initial sequent for any n. As we stipulated A does not contain exp, the latter formula will be A^n. The proof is now the same as Theorem 10. $\Box$

Theorem 14 *If $I\Delta_0{+}exp \vdash FCFCon(IOpen(f))$, then $IOpen(exp, f) \neq I\Delta_0{+}exp$.*

PROOF. This follows from Lemma 10 by the same proof as Theorem 12. $\Box$

5 Acknowledgements

The author would like to thank the referee for his suggestions on how to streamline this paper.

References

[1] J .H. Bennett. *On Spectra*. PhD thesis, Princeton University, 1962.

[2] S.R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.

[3] S.R. Buss. Algorithms for boolean formula evaluation and tree contraction. In S.R. Buss, editor, *Handbook of Proof Theory*, pages 79–147. North Holland, 1998.

[4] S.R. Buss. Bounded arithmetic, complexity and cryptography. *To appear Theoria*, 1998.

[5] P. Clote and G. Takeuti. Exponential time and bounded arithmetic (extended abstract). In *Structure in Complexity Theory LNCS223*, pages 125–143. Springer-Verlag, 1986.

[6] H. Gaifman and C. Dimitracopoulos. Fragments of Peano's arithmetic and the MRDP theorem. In *Proceedings of the Eighteenth Annual ACM Symposium on theory of Computing*, Monographie 30 de L'Enseignement Math'ematique, pages 187–206, 1980.

[7] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetics*. Springer-Verlag, 1993.

[8] R. Kaye. *Diophantine and parameter free induction*. PhD thesis, Manchester University, 1987.

[9] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press, 1995.

[10] C. Pollett. Multifunction algebras and the provability of PH⇓. To appear Annals of Pure and Applied Logic.

[11] C. Pollett. Structure and definability in general bounded arithmetic theories. *Annals of Pure and Applied Logic*, 100:189–245, 1999.

[12] C. Pollett. *Arithmetic Theories with Prenex Normal Form Induction*. PhD thesis, University of California, San Diego, 1997.

[13] J.C. Shepherson. Non-standard models for fragments of number theory. In *The Theory of Models (Studies in Logic Found. Math.)*, pages 343–358. North Holland, 1965.

[14] G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 364–386. Oxford Science Publications, 1993.

[15] A. Wilkie and J. Paris. On the scheme of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, 35:261–302, 1987.

[16] G.M. Wilmers. Bounded existential induction. *Journal of Symbolic Logic*, 50:72–90, 1985.